Simplified AES

Example

Steven Gordon

1 Simplified AES Example

Lets assume the inputs for the encryption are:

- 16-bit Plaintext, *P*: 1101 0111 0010 1000
- 16-bit Key, *K*: 0100 1010 1111 0101

1.1 Key Generation

The first step is to generate the sub-keys. This is called *Key Generation* or *Key Expansion*:

The input key, *K*, is split into 2 words, w_0 and w_1:

w_0 = 0100 1010
w_1 = 1111 0101

The first sub-key, Key_0, is in fact just the input key: $Key_0 = w_0 w_1 = K$

The other sub-keys are generated as follows:

w_2 = w_0 XOR 10000000 XOR SubNib(RotNib(w_1))

(Note: RotNib() is “rotate the nibbles”, which is equivalent to swapping the nibbles)

= 0100 1010 XOR 10000000 XOR SubNib(0101 1111)

(Note: SubNib() is “apply S-Box substitution on nibbles using encryption S-Box”)

= 1100 1010 XOR SubNib(0101 1111)
= 1100 1010 XOR 0001 0111
= 1101 1101

w_3 = w_2 XOR w_1
= 1101 1101 XOR 1111 0101
= 0010 1000

w_4 = w_2 XOR 0011 0000 XOR SubNib(RotNib(w_3))
= 1101 1101 XOR 0011 0000 XOR SubNib(1000 0010)
= 1110 1101 XOR 0110 1010
= 1000 0111

w_5 = w_4 XOR w_3
= 1000 0111 XOR 0010 1000
= 1010 1111

Now the sub-keys are:

Key_0 = w_0w_1
= 0100 1010 1111 0101

Key_1 = w_2w_3
= 1101 1101 0010 1000

Key_2 = w_4w_5
= 1000 0111 1010 1111

1.2 Encryption

Now let’s do the encryption. There is an initial operation (Add Round Key), followed by the main Round, followed by the final Round. (Note, the main difference in the real DES is that the main Round is repeated many times).

Remember, the output of each operation is used as the input to the next operation, always operating on 16-bits. The 16-bits can be viewed as a state matrix of nibbles.

1.2.1 Add Round 0 Key

Plaintext XOR Key_1
= 1101 0111 0010 1000 XOR
0100 1010 1111 0101
= 1001 1101 1101 1101

1.2.2 Round 1

Nibble Substitution (S-boxes). Each nibble in the input is used in the Encryption S-Box to generate an output nibble.

Input = 1001 1101 1101 1101
Output = 0010 1110 1110 1110

Shift Row. Swap 2nd nibble and 4th nibble (note, in this example, its not so easy to see since 2nd and 4th nibbles are the same!)

= 0010 1110 1110 1110

Mix Columns. Apply the matrix multiplication with the constant matrix, M_e, using GF(2^4). For GF(2^4), the addition operation is simply an XOR, and for the multiplication operation you can use a lookup table.

$$M_e = \begin{matrix} 1 & 4 \\ 4 & 1 \end{matrix}$$

$$S = \begin{matrix} 0010 & 1110 \\ 1110 & 1110 \end{matrix} = \begin{matrix} S_{00}' & S_{01}' \\ S_{10}' & S_{11}' \end{matrix}$$

$$\begin{aligned} S' &= M_e \text{ x } S \end{aligned}$$

$$\begin{aligned} S_{00}' &= \text{0010 XOR (4 x 1110)} \\ &= \text{0010 XOR (4 x E)} \\ &= \text{0010 XOR D} \\ &= \text{0010 XOR 1101} \\ &= \text{1111} \end{aligned}$$

$$\begin{aligned} S_{10}' &= \text{(4 x 0010) XOR 1110} \\ &= \text{1000 XOR 1110} \\ &= \text{0110} \end{aligned}$$

$$\begin{aligned} S_{01}' &= \text{1110 XOR (4 x 1110)} \\ &= \text{1110 XOR (4 x E)} \\ &= \text{1110 XOR 1101} \\ &= \text{0011} \end{aligned}$$

$$\begin{aligned} S_{11}' &= \text{(4 x 1110) XOR 1110} \\ &= \text{1101 XOR 1110} \\ &= \text{0011} \end{aligned}$$

$$\begin{aligned} \text{Output} &= S_{00}'\ S_{10}'\ S_{01}'\ S_{11}' \\ &= \text{1111 0110 0011 0011} \end{aligned}$$

Add Round 1 Key.

$$\begin{aligned} &= \text{1111 0110 0011 0011 XOR} \\ & \text{1101 1101 0010 1000} \\ &= \text{0010 1011 0001 1011} \end{aligned}$$

1.2.3 Final Round

Nibble Substitution (S-boxes)

= 1010 0011 0100 0011

Shift Row (2nd and 4th)

= 1010 0011 0100 0011

Add Round 2 Key

$$\begin{aligned} & \text{1010 0011 0100 0011 XOR} \\ & \text{1000 0111 1010 1111} \\ &= \text{0010 0100 1110 1100} \end{aligned}$$

Now we have the final ciphertext.

Ciphertext = 0010 0100 1110 1100

1.3 Decryption

Now lets decrypt. Note that we use the same keys generated during the encryption (that is, the decryptor would generate the round sub-keys using the input key K, *using the encryption S-Box*).

Add Round 2 Key

0010 0100 1110 1100 XOR
1000 0111 1010 1111
= 1010 0011 0100 0011

Inverse Shift Row (same as normal)

= 1010 0011 0100 0011

Inverse Nibble Sub (use the inverse or decryption S-box)

= 0010 1011 0001 1011

Add Round 1 Key

= 0010 1011 0001 1011 XOR
1101 1101 0010 1000
= 1111 0110 0011 0011

Inverse Mix Columns

$$S = \begin{matrix} S_{00} & S_{01} \\ S_{10} & S_{11} \end{matrix}$$

$$= \begin{matrix} 1111 & 0011 \\ 0110 & 0011 \end{matrix}$$

$$S' = \begin{matrix} S_{00}' & S_{01}' \\ S_{10}' & S_{11}' \end{matrix}$$

$$= \begin{matrix} 9 \text{ x } S_{00} \text{ XOR } 2 \text{ x } S_{10} & 9 \text{ x } S_{01} \text{ XOR } 2 \text{ x } S_{11} \\ 2 \text{ x } S_{00} \text{ XOR } 9 \text{ x } S_{10} & 2 \text{ x } S_{01} \text{ XOR } 9 \text{ x } S_{11} \end{matrix}$$

S_{00}' = (9 x 1111) XOR (2 x 0110)
= 9 x F XOR 2 x 6
= E XOR C
= 1110 XOR 1100
= 0010

S_{10}' = 2 x 1111 XOR 9 x 0110
= 2 x F XOR 9 x 6
= D XOR 3
= 1101 XOR 0011
= 1110

S_{01}' = 9 x 0011 XOR 2 x 0011
= 9 x 3 XOR 2 x 3
= 8 XOR 6
= 1000 XOR 0110
= 1110

S_{11}' = 2 x 0011 XOR 9 x 0011
= 1110

Output = 0010 1110 1110 1110

Inverse Shift Row
= 0010 1110 1110 1110

Inverse Nibble Sub
= 1001 1101 1101 1101

Add Round 0 Key
= 1001 1101 1101 1101 XOR
0100 1010 1111 0101
= 1101 0111 0010 1000

Plaintext = 1101 0111 0010 1000

Original = 1101 0111 0010 1000

The decryption worked!